tenable® network security

Nessus® professional

Product Overview

Nessus, the industry's most widely deployed vulnerability scanner helps you reduce your organization's attack surface and ensure compliance in physical, virtual, mobile and cloud environments. Nessus features high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery and vulnerability analysis. With the world's largest continuously-updated library of vulnerability and configuration checks, and the support of Tenable's expert vulnerability research team, Nessus sets the standard for speed and accuracy.

Nessus supports more technologies than competitive solutions, scanning operating systems, network devices, hypervisors, databases, tablets, phones, web servers and critical infrastructure for vulnerabilities, threats and compliance violations.

Nessus allows the user to sort and filter vulnerability findings using over 20 different criteria. Severity ratings can be customized and the remediation summary provides actionable results.

Nessus Features

Reporting and Monitoring

- Flexible reporting: Customize reports to sort by vulnerability or host, create an executive summary, or compare scan results to highlight changes
  - Native (XML), PDF (requires Oracle Java be installed on Nessus server), HTML and CSV formats
- Targeted email notifications of scan results, remediation recommendations and scan configuration improvements
- Results/report sharing (requires Nessus Manager)

Scanning Capabilities

- Discovery: Accurate, high-speed asset discovery
- Scanning: Vulnerability scanning (including IPv4/IPv6/hybrid networks)
  - Un-credentialed vulnerability discovery
  - Credentialed scanning for system hardening & missing patches
- Coverage: Broad asset coverage and profiling
  - Network devices: firewalls/routers/switches (Juniper, Check Point, Cisco, Palo Alto Networks), printers, storage
  - Offline configuration auditing of network devices
  - Virtualization: VMware ESX, ESXi, vSphere, vCenter, Hyper-V, and Citrix Xen Server

With more than 20,000 customers worldwide, Nessus is trusted by more professionals than any other security and compliance product.

Complete Vulnerability Coverage:

- Virtualization & cloud
- Malware & botnets
- Configuration auditing
- Web applications

Key Benefits

- Custom fit for your environment:
  - Flexible deployment, scanning and reporting
  - Email notifications of scan results and remediation recommendations
  - Custom vulnerability severity ratings
- Identify malware, botnets and malicious processes
- Lower your cyber risks, vulnerabilities and material violations during audits
  - Dynamic scan results
- Low total cost of ownership (TCO)
  - part of subscription
  - engine, UI, plugins, policies, scan templates
  - Nessus subscriptions include software updates, access to compliance and audit files, and support
  - Automatic plugin, engine and user-interface updates
- Anytime, anywhere access from an Internet browser for improved efficiency

  - Operating systems: Windows, Mac, Linux, Solaris, BSD, Cisco iOS, IBM iSeries
  - Databases: Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL, MongoDB
  - Web applications: Web servers, web services, OWASP vulnerabilities
  - Cloud: Scans cloud applications and instances like Salesforce and AWS
  - Compliance: Helps meet government, regulatory and corporate requirements
  - Meets PCI DSS requirements through configuration auditing, web application scanning
- Threats: Botnet/malicious, process/anti-virus auditing
  - Detect viruses, malware, backdoors, hosts communicating with botnet-infected systems, known/unknown processes, web services linking to malicious content
  - Compliance auditing: FFIEC, FISMA, CyberScope, GLBA, HIPAA/HITECH, NERC, PCI, SCAP, SOX
  - Configuration auditing: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA
- Control Systems Auditing: SCADA systems, embedded devices and ICS applications
- Sensitive Content Auditing: PII (e.g. credit card numbers, SSNs)

Deployment and Management

- Flexible deployment: software, hardware, virtual appliance deployed in service provider's cloud, or as a Tenable hosted cloud service (Nessus Cloud).
- Scan options: Agent-based and Agentless scanning for easy deployment and maintenance. Supports both non-credentialed, remote scans and credentialed, local scans for deeper, granular analysis of assets that are online as well as offline or remote.
- Configuration/policies: Out-of-the-box policies and configuration templates.
- Risk scores: Vulnerability ranking based on CVE, five severity levels (Critical, High, Medium, Low, Info), customizable severity levels for recasting of risk.
- Prioritization: Correlation with exploit frameworks (Metasploit, Core Impact, Canvas, and ExploitHub) and filtering by exploitability and severity.
- Extensible: RESTful API support for integrating Nessus into your existing vulnerability management workflow.

The Nessus Advantage

Customers choose Nessus because it offers:

- Highly-accurate scanning with low false positives
- Comprehensive scanning capabilities and features
- Scalable to hundreds-of-thousands of systems
- Easy deployment and maintenance
- Low cost to administer and operate
- Complete coverage with Agents, including laptops and mobile assets

Training and Certification

Nessus training and certification are available for those who are new to using Nessus and want the knowledge and skills to maximize every benefit of the Nessus scanner. Tenable offers both On-Demand Training and Certification Exams which are available separately or combined with subscriptions for Nessus, Nessus Manager, or Nessus Cloud.

Taking Nessus to the Next Level

Nessus can now be used with the following Tenable solutions to achieve team-oriented vulnerability scanning and remediation goals:

Nessus Manager

Nessus Manager provides collaboration and centralized administration over multiple scanners. Engage system/network administrators, forensics & incident response teams, risk & compliance, and desktop support in the vulnerability management process. The industry's most widely deployed vulnerability and configuration assessment product now offers role-based sharing of scanners, policies, schedules and scan results among an unlimited set of users.

Nessus Cloud

Tenable-hosted version of Nessus features Nessus scanning capabilities, resource sharing and role-based access control for multiple users from a remote, cloud-based solution. Nessus Cloud can also be used to satisfy external, quarterly network scanning requirements for PCI. Nessus Cloud is a PCI-Certified Approved Scanning Vendor (ASV) solution. Scan your perimeter today!

Complementary Tenable Products

Organizations can extend the capabilities of Nessus Manager with these complementary products from Tenable:

SecurityCenter™ Continuous View

SecurityCenter Continuous View is Tenable's market-defining continuous monitoring platform, allowing for the most comprehensive and integrated view of network health across all environments, including traditional, mobile, virtual and cloud. It provides a unique combination of detection, reporting and pattern recognition utilizing industry-recognized algorithms and models to deliver the most advanced analysis of security risks and compliance exposure. Using SecurityCenter Continuous View, users can eliminate risk, rapidly respond to advanced threats and compliance violations, and identify failing security processes.

tenable® network security

For More Information: Please visit tenable.com
Contact Us: Please email us at subscriptionsales@tenable.com or visit tenable.com/contact